



Installation Guide

McAfee SaaS Endpoint Protection 6.0

COPYRIGHT

Copyright © 2012 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS

McAfee, the McAfee logo, McAfee Active Protection, McAfee AppPrism, McAfee Artemis, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Enterprise Mobility Management, Foundscore, Foundstone, McAfee NetPrism, McAfee Policy Enforcer, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, SmartFilter, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure, WormTraq are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface	5
About this guide	5
Audience	5
Conventions	5
What's in this guide	6
Find product documentation	6
 1 Installing McAfee SaaS Endpoint Protection	 9
After you place your order	10
Merge multiple orders	10
System requirements	11
Browser requirements	11
Operating system requirements	11
RAM requirements	12
Requirements for SaaS email protection	13
Requirements for email server protection	13
Advanced network environments	14
Prepare for installation	16
Uninstall active virus protection software	16
Uninstall active firewall software	16
Perform optional checks and preventive maintenance	16
Install the standalone installation agent	17
Summary of installation methods	18
The standard URL installation process	19
Requirements for URL installation	19
Install the software on the administrative computer	19
Send an installation URL to users	20
Install the software on a client computer	20
The silent installation process	22
Requirements for silent installation	22
Install with silent installation	22
Designate a relay server with VSSETUP	23
VSSETUP parameters	24
The push installation process	25
Requirements for push installation	26
Considerations for scheduling push installations	26
Install with push installation	27
Processes for pre-installed and CD versions	28
About pre-installed trial and full subscriptions	28
When you first turn on the computer	29
Activate the software	29
Purchase or renew a full subscription	29
View or create an account enrollment key	30
Activate your license key after installation	30
Complete the installation	31

Test virus protection	31
Scan the client computer	31
Scan the email Inbox	32
2 Troubleshooting and reference	33
Troubleshooting tasks	33
Troubleshoot general installation problems	33
Uninstall the client software	34
Frequently asked questions	35
Error messages	36
Index	39

Preface

This guide provides the information you need to install your McAfee product.

Contents

- [About this guide](#)
- [Find product documentation](#)

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses the following typographical conventions and icons.

Book title or Emphasis Title of a book, chapter, or topic; introduction of a new term; emphasis.

Bold Text that is strongly emphasized.

User input or Path Commands and other text that the user types; the path of a folder or program.

`Code` A code sample.

User interface Words in the user interface including options, menus, buttons, and dialog boxes.

Hypertext blue A live link to a topic or to a website.

 **Note:** Additional information, like an alternate method of accessing an option.

 **Tip:** Suggestions and recommendations.

 **Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.

 **Warning:** Critical advice to prevent bodily harm when using a hardware product.

What's in this guide

This guide is organized to help you find the information you need.

- System requirements
- Tasks to perform before installation
- Installation tasks:
 - Using an installation URL
 - Using the VSSETUP silent installation utility
 - Using the push installation utility
- Tasks to perform after installation is complete
- Reference and troubleshooting information

Other product documents

Context-sensitive online Help is available on any page of the SecurityCenter by clicking the help link (?) in the upper-right corner.

These product documents are also available:

Document	How to access
Product guide	From the SecurityCenter, click the link on the Help & Support tab.
Release notes	From the SecurityCenter, click the link on the Help & Support tab.  Release notes are available for the most recent release of the client software and the most recent upgrade of SaaS protection services and SecurityCenter features.
Push installation online Help	During a push installation, click the help link in any dialog box.
Client installation online Help	During a standard installation on a client computer, click the help link in any dialog box.
Client online Help	From the client console on a client computer, select Action Menu View Help .
SaaS extension quick start guide SaaS extension troubleshooting guide	From the SecurityCenter, click the link on the ePO Servers tab of the Utilities page. These short guides provide information on installing and using the McAfee® Security-as-a-Service extension for McAfee® ePolicy Orchestrator.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

- 1 Go to the McAfee Technical Support ServicePortal at <http://mysupport.mcafee.com>.
- 2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click Product Documentation. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click Search the KnowledgeBase for answers to your product questions. • Click Browse the KnowledgeBase for articles listed by product and version.

1

Installing McAfee SaaS Endpoint Protection

This document describes what happens after you purchase the product, provides system requirements information, and explains how to install the software on client computers.



Some of the protection services managed by McAfee® SaaS Endpoint Protection do not require software to be installed on client computers. Refer to emails and materials from McAfee for instructions on setting them up. Examples include the McAfee SaaS protection services and the email server protection service.

Contents

- ▶ *After you place your order*
- ▶ *System requirements*
- ▶ *Prepare for installation*
- ▶ *Summary of installation methods*
- ▶ *The standard URL installation process*
- ▶ *The silent installation process*
- ▶ *The push installation process*
- ▶ *Processes for pre-installed and CD versions*
- ▶ *Complete the installation*

After you place your order

When you place an order for McAfee SaaS Endpoint Protection, you supply an email address. Your account is associated with that email address, and McAfee sends verification and other correspondence about your account to that address.

After you submit your order:

- 1 McAfee processes your order.
- 2 You receive up to three messages.

This email...	Contains...
Welcome	The download URL and instructions for installing the client software, accessing documentation, and contacting customer support. For most customers, the welcome email also includes a grant number for the order, which is required for customer support.
Logon credentials	Instructions for logging on to the McAfee® SecurityCenter administrative website and changing your password.
Grant letter (optional)	The grant number for the order, which is required for customer support. Your service provider determines whether you receive a grant letter.

- 3 With some services, you receive additional instructions for configuring required settings and logging on to associated portals.



If you purchase the product from a McAfee partner who manages security for you, the partner usually receives these emails. If you have questions about which emails you should receive, contact the partner.

Merge multiple orders

If you placed more than one order using different email addresses, you have more than one account.

Use this task from the SecurityCenter to merge separate accounts so that all your security information and emails are sent to a single email address.

Task

For option definitions, click ? in the interface.

- 1 On the **My Account** page, click the **Accounts & Keys** tab.
- 2 In the **Manage Accounts** section, select **Merge another account**.
- 3 On the **Step 1** page, enter the email address and password activated for the account you want to merge into your main account, then click **Next**.
- 4 On the **Step 2** page, view details for the account you have selected. Verify that the licenses and computers listed for the account are the ones you want to merge, then click **Next**.
- 5 On the **Step 3** page, click **Merge Account**.

System requirements

Before installing the client software, verify that client computers meet these requirements.

General requirements

- Intel Pentium processor or compatible architecture



Check the Microsoft website for requirements that are specific to each operating system. For example, Windows 2008 Server requires at least a 1 GHz (x86) or 1.4 GHz (x64) processor.

- Microsoft mouse or compatible pointing device
- 256-color or higher VGA monitor

For a current list of system requirements, visit <http://www.mcafee.com/us/products/saas-endpoint-protection-suite.aspx>.

Browser requirements

Installation requires an Internet connection and a supported web browser.

Product features have been verified to function correctly on these versions of popular browsers:

- Microsoft Internet Explorer (versions 7, 8, 9, and 10)
- Mozilla Firefox (versions 3.0 through 15)
- Google Chrome (versions 4.0 through 21)
- Apple Safari for Windows (version 4.0, 5.0, and 5.1) (browser protection service features not supported)

The installation wizard works with the default security level for Internet Explorer. For other browsers, select a security level that enables Javascript. See the web browser's documentation for instructions on configuring the security level if you need to change it.

A supported browser is also required to access features on the SecurityCenter.

Operating system requirements

The computers where you want to install the software must be running a supported operating system.

These protection services include client software:

- Virus and spyware protection
- Firewall protection
- Browser protection and content filtering module

Requirements for other protection services appear elsewhere in this document.

Client operating systems

- Microsoft Windows 8 (32-bit or 64-bit)
- Microsoft Windows 7 (32-bit or 64-bit): Ultimate, Professional, Home Premium, Home Basic

- Microsoft Windows Vista (32-bit or 64-bit): Ultimate, Enterprise, Business, Home Premium, Home Basic
- Windows XP with Service Pack 2 or 3 (32-bit and 64-bit): Home or Professional



The firewall protection service is not supported on computers running 64-bit versions of Windows XP.

Server operating systems

- Windows Server 2012
- Windows Server 2011: Small Business Server
- Windows Server 2008 R2: Standard, Enterprise
- Windows Server 2008 (32-bit and 64-bit): Standard, Enterprise, Small Business Server
- Windows Small Business Server 2003 R2
- Windows Server 2003 with Service Pack 1 (32-bit and 64-bit): Standard, Enterprise, Small Business Server

Notify users when support ends

By default, the client software displays notifications to remind users that support is ending for their operating system.

- When upgrades to product components, such as the scanning engine, are scheduled to end or will end within 30 days.
- When updates to detection definition (DAT) files have ended or will end within 30 days.

A policy option determines whether support notifications are displayed.



Notifications are not displayed for computers running versions of Windows for which support has already ended.

Use this task to enable or disable automatic notifications.

Task

For option definitions, click ? in the interface.

- 1 In the SecurityCenter, click the **Policies** tab, then click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Click **Client Settings**.
- 3 On the **Client Settings** tab, under **Display Settings**, select or deselect **Display support notifications**.
- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

RAM requirements

Before installing the client software, use this table to verify that sufficient RAM is installed on client computers.

Operating system	Minimum for single protection service	Minimum for multiple protection services	Recommended
Windows XP	512 MB	1 GB	1 GB
Windows 2003	512 MB	1 GB	2 GB

Operating system	Minimum for single protection service	Minimum for multiple protection services	Recommended
Windows Vista	1 GB	1 GB	2 GB
Windows 7	1 GB	1 GB	2 GB
Windows 8	1 GB	1 GB	2 GB
Windows Server 2008	512 MB	1 GB	2 GB
Windows Small Business Server 2011	2 GB	2 GB	4 GB
Windows Server 2012	1 GB	1 GB	2 GB
Other Servers	512 MB	1 GB	2 GB



When calculating the total RAM required, consider the memory requirements of other software applications running on client computers.

Requirements for SaaS email protection

To set up and run the SaaS email protection service, you need to have set up these required components.

- A dedicated email server, either in-house or hosted by an ISP.
- A company email domain, such as yourdomain.com, with a static IP address.

Instructions for activating and setting up the SaaS email protection service are provided in an email from McAfee and in the product guide.



You must have your own domain name pointing to your own email server or a server hosted by a service provider. We cannot provide this service for email accounts on major services such as Yahoo or Google, because these providers control their own domains. If you attempt to activate the SaaS email or web protection service by using an unsupported domain name, you will be notified that the domain is not accepted. Unsupported domain names include major domains such as gmail.com, yahoo.com, mcafee.com, and hotmail.com.

Requirements for email server protection

Before installing the email server protection service, verify that your email server is running a supported operating system and meets or exceeds minimum requirements.

Email server protection supports these versions of Microsoft Exchange:

- Microsoft Exchange Server 2007 with Service Pack 2 or 3
- Microsoft Exchange Server 2003 with Service Pack 2

Email server protection also supports Lotus Domino running on these operating systems:

- Windows 2008 Server with Service Pack 2
- Windows 2003 Enterprise Server with Service Pack 2
- Windows 2003 Server

For detailed information about system requirements, see <http://www.mcafee.com/us/products/security-for-email-servers.aspx>.

Instructions for installing the email server protection service are provided in emails and materials from McAfee.

Advanced network environments

Check the following table for any special considerations that apply to your network.

If your network includes...	Check this topic
One or more computers without an Internet connection	<i>Decide whether to set up relay servers</i>
Computers running the Windows firewall	<i>How firewall protection interacts with the Windows firewall</i>
A corporate firewall or proxy server	<i>Support for corporate firewalls or proxy servers</i>
Terminal servers or shared computers where the fast user switching feature is used	<i>Terminal server support</i>
Active Directory groups	<i>Active Directory support</i>

Decide whether to set up relay servers

Before installing the client software, decide whether you want to set up relay servers and which computers should be relay servers. This affects which installation methods you can use for these computers.

When to set up relay servers

It is not necessary to set up relay servers. However, you might want to consider designating one or more computers as relay servers if any computers on your network do not have a direct connection to the Internet.

What is a relay server?

The Internet Independent Updating (IIU) feature allows computers without an Internet connection to receive software updates through another local computer that has been designated as a relay server. Any computer with an Internet connection can be set up as a relay server at the time the client software is installed or at a later time. A relay server acts as a proxy for other computers by allowing them to use its connection to check for updates.

How to set up relay servers

Specify relay servers using these methods:

- Silent installation — Designate a relay server during installation, or run VSSETUP at any time to reconfigure a client computer as a relay server.
- Push installation — Designate a relay server during installation.

How firewall protection interacts with the Windows firewall

To ensure complete protection on computers running Windows XP, Windows Vista, Windows 7, or Windows 8 firewall protection automatically disables the Windows firewall and configures itself as the

default firewall. This enables it to monitor communications for Internet applications and track events for reporting purposes, even if the Windows firewall is also running.

We recommend that you do not re-enable the Windows firewall while the firewall protection service in McAfee SaaS Endpoint Protection is enabled.



If both firewalls are enabled, the firewall protection service firewall lists only a subset of the blocked IP addresses in its **Inbound Events Blocked by the Firewall** report. The Windows firewall blocks some of these addresses; however, it does not report them because event logging is disabled in the Windows firewall by default. If both firewalls are enabled, you must enable Windows firewall logging to view a list of all blocked IP addresses. The default Windows firewall log is C:\Windows\pfirewall.log. Enabling both firewalls also results in duplicate status and alert messaging.

Support for corporate firewalls or proxy servers

The client software downloads components directly from McAfee servers to client computers. If you are behind a corporate firewall, or are connected to the Internet by a proxy server, you might need to provide additional information for your service to work properly.

- Authentication support is limited to anonymous authentication or Windows domain challenge/response authentication. Basic authentication is not supported.
- Silent installation, push installation, and automatic updating do not support a CHAP or NTLM proxy.

Contact the site administrator or product support if you have proxy questions while installing or updating the client software.

Terminal server support

McAfee SaaS Endpoint Protection supports terminal servers and the Windows fast user switching feature in most scenarios, with these limitations:

- The client software must be installed on the server by someone with local administrator rights.
- When an installation or update occurs on a terminal server, one session is designated as the primary update session. A pseudo user is defined, which enables automatic updates to occur on computers where no user is logged on. See the product guide for more information.
- For all user sessions, the product icon is removed from the system tray during the installation or update. The icon is restarted after the update.

Active Directory support

If you use Active Directory to define group hierarchies in your network, you can deploy the client software directly to your Active Directory groups.

Before installing, you need to log on to the SecurityCenter, download the Active Directory Synchronization utility from the **Utilities** page, and import the organizational unit (OU) structure for your network into the SecurityCenter. You can then install the client software on computers in your Active Directory groups. See the product guide, available from the **Help & Support** page of the SecurityCenter, for more information.

Prepare for installation

Use these tasks to prepare a client computer before installing the client software.

Uninstall active virus protection software

Other virus protection software might conflict with the advanced features of the virus and spyware protection service. When multiple virus scanning engines try to access the same files on your computer, they interfere with each other.

The installation wizard detects existing virus protection products during installation. It can uninstall some of these products for you, and it prompts you to uninstall other products manually. If you are notified of existing virus protection software on a computer during installation, you must uninstall it before installing the virus and spyware protection service.

Use this task to uninstall existing virus protection software before installing the virus and spyware protection service. (There is no need to uninstall an existing installation of the virus and spyware protection service.)

For a list of software that is detected and/or uninstalled during installation, visit http://www.mcafeesasap.com/downloads/uninstallinfo/detected_software_list.html

Task

- 1 In the Windows Control Panel, open **Add/Remove Programs** or **Programs and Features**.
- 2 From the list of programs, select any virus protection software, then click **Remove** or **Uninstall**.

Uninstall active firewall software

Before installing firewall protection, we recommend that you uninstall any other firewall programs on your computer. (There is no need to uninstall an existing installation of McAfee SaaS Endpoint Protection.) Follow your firewall program's instructions for uninstalling or use the Windows Control Panel.

Use this task to uninstall existing firewall software from the Windows Control Panel.

Task

- 1 In the Windows Control Panel, open **Add/Remove Programs** or **Programs and Features**.
- 2 From the list of programs, select any firewall software, then click **Remove** or **Uninstall**.



On computers running the Windows firewall, it is disabled automatically during installation of the firewall protection service.

Perform optional checks and preventive maintenance

Perform this optional task to avoid some pitfalls that can occur during installation.

The installation wizard checks for compliance with some of the minimum requirements before installing the software. If any of these requirements is not met, it displays a notification and cancels the installation.

If you do not have...	Then do this...
Administrative rights on the computer	Ask your administrator to assign administrator rights to you or to install the standalone installation agent.
Sufficient available disk space	Make at least 300 MB of disk space available, then begin the installation process again.

If you do not have...	Then do this...
A supported browser	Begin the installation process again using one of the supported browsers.
A supported operating system	Install the software on a computer running one of the supported operating systems.

These additional precautions minimize issues that can lead to installation problems.



For a comprehensive set of automated pre-installation checks, you can download and run the pre-installation utility. It performs all the steps listed below and more. See [KB75738](#) for the downloadable file and instructions for using it.

Task

- 1 Check to ensure your computer meets these basic requirements.

Do you have...	Comments
The browser security setting set appropriately?	The installation wizard works with the default security level for Internet Explorer. For other browsers, select a security level that enables Javascript.
The minimum amount of RAM required?	The installation wizard checks for RAM, but does not cancel the installation process if the computer doesn't meet the minimum requirement. If installation fails and you do not meet minimum RAM requirements, increase the amount of RAM, then begin the installation process again.

- 2 Empty the browser cache, including temporary Internet files.

See the browser's documentation for instructions. For most browsers, you can access this feature by using the **Tools** or **Tools | Options** menu option.

- 3 Check your connection to the Internet and the installation site.

Make sure the computer can access <http://www.mcafeesasap.com>.

See also

[RAM requirements on page 12](#)

Install the standalone installation agent

To allow users without local administrator rights to install the client software by using a URL, you must first load a standalone installation agent on their client computers.



This is an optional task that is required *only* for a user without administrator rights to install the client software on a client computer.

Use this task to install the installation agent by using a deployment tool or by downloading it directly onto client computers. You must have administrator rights on the client computer to install this file. After the standalone installation agent is installed, any user can install the client software on that computer.

Task

- Use one of these procedures to deploy the standalone installation agent to a client computer.

From this location...	Follow these steps...
The administrative computer	1 From the SecurityCenter website, click the Utilities tab. 2 Click the Installation tab, then in the Installation section click Download. 3 Deploy and execute the file on client computers using your customary deployment tools, such as Microsoft Systems Management Server (SMS) installer, Windows NT login scripts, or Tivoli IT Director.
The client computer	1 From the SecurityCenter website, click the Utilities tab. 2 Click the Installation tab, then in the Installation section click Download. 3 When the download is complete, double-click the file.

Summary of installation methods

There are three methods for installing the client software.

Standard URL installation

Use the URL you received in your welcome email message to install the software on your computer and access the SecurityCenter website. Then install the software on other computers by using a standard or customized URL, or send the URL to users with instructions on how to install.

Advanced installation options

From an administrative computer, visit the SecurityCenter and select an advanced installation method to remotely install the software on one or more computers simultaneously without user interaction.

- **Silent installation** — Download a program called VSSETUP.EXE, then run it at the command line. This method requires a third-party deployment tool, a login script, or a link to an executable file in an email message.
- **Push installation** — Download the Push Install utility, then deploy the software directly from your service provider's website.

This table summarizes the differences in the advanced installation methods.

The administrator...	Advanced installation method	
	Silent	Push
Performs the installation from	Client computer	Administrative computer
Downloads this file	VSSETUP.EXE	Push Install utility
Installs the client software on	One computer	One or more computers
Installs remotely	No	Yes
Can designate relay servers (optional)	Yes	Yes (separately from client computer)
Can deploy to Active Directory groups		Yes

The standard URL installation process

URL installation is the most common installation method. Client software is installed on each computer individually. Users install the client software by downloading it to their computers from a company-specific URL.

How URL installation works

- 1 Obtain your download URL from your welcome email message or create a customized URL from the SecurityCenter.
- 2 Send the URL to users in an email message with instructions on how to install. (*Optional*)
- 3 From the client computer, enter the URL into a browser window.

Requirements for URL installation

Make sure client computers meet the basic requirements for installing the client software by using a URL.

- The client computer must have an Internet connection.
- A supported web browser must be installed and configured correctly.
- The client computer's user must have local administrator rights.



Administrator rights are not the default setting. Change the default Windows configuration or deploy a standalone installation agent on the client computer.

See also

[System requirements on page 11](#)

[Install the standalone installation agent on page 17](#)

Install the software on the administrative computer

Use this task to install the client software directly on the computer used by the administrator.

To install all the protection services in your subscription with their default settings, open the welcome email sent to you by McAfee, then click the installation URL or copy and paste it into a web browser on your computer.

This task lets you specify customized settings or install from the SecurityCenter.

Task

For option definitions, click ? in the interface.

- 1 In your web browser, log on to the SecurityCenter.
- 2 From the **Dashboard** or **Computers** page, click **Install Protection**.
- 3 Select **Desktop protection**, then click **Next**.
- 4 Select **Install on this computer**.
- 5 Select the appropriate options:
 - The group in which to place the client computers
 - The policy to assign to the computers

- The protection services to install
- The language for the software

6 Click **Click here to install**.

Send an installation URL to users

As the administrator, you can obtain the company-specific installation URL in two ways.

- When you subscribe to McAfee SaaS Endpoint Protection, you receive an email message containing the URL that has been set up for your company. This installation URL installs the protection services you have subscribed to into your account's default group in your account's default language. You can copy this URL into an email message to send to other computer users at your company.
- At any time, you can log on to the SecurityCenter and create a customized URL to send to users. This enables them to install selected protection services in a designated group and language.

Use this task to create a customized installation URL and send it to users.

Task

For option definitions, click ? in the interface.

- 1 In your web browser, log on to the SecurityCenter.
- 2 From the **Dashboard** or **Computers** page, click **Install Protection**.
- 3 Select **Desktop protection**, then click **Next**.
- 4 Select **Obtain a URL for installing on other computers**.
- 5 Select the appropriate options:
 - The group in which to place the client computers
 - The policy to assign to the computers
 - The protection services to install
 - The language for the software
- 6 Click **Get URL**.

A customized URL is displayed, along with simple instructions for users.
- 7 Click **Select Text and Copy to Clipboard**, then click **Email**.

An email message opens in your local email application. The text and URL you copied appears in the message.
- 8 Type email addresses into the message, revise the instructions if needed, then click **Send**.

Install the software on a client computer

Use this task to install the client software with a URL.

Before you begin

McAfee or the site administrator has sent the installation URL to the computer in an email message, and you have performed the tasks required to prepare the computer for installation.

When installation is complete, the software downloads the detection definition (DAT) files in the background. This allows you to get back to work without having to wait for a lengthy download to complete.



The computer is not fully protected until the DAT files are downloaded. Be sure not to turn off the computer or disconnect the Internet connection until the download is complete.

Task

For option definitions, click ? in the interface.

- 1 Open the email message on the client computer.
- 2 Select the URL or copy and paste it into a browser window to begin installation.
When entering the URL into a browser, make sure to enter the entire URL without spaces.
- 3 Select the protection services to install if you are prompted to do so, type your email address in the **Email or identifier** field, and click **Continue**.



The information entered here identifies the computer in reports. If reports indicate a problem with the computer, the administrator uses the email address to notify the person who uses the computer. If you do not enter an email address, it is important that the administrator knows the correct contact information.

- 4 When you are prompted to do so, click **Install**.
- 5 In the **File Download** dialog box, click **Run**.
- 6 Click **Yes** or **Continue** if you are prompted to allow the software to make changes to your computer.
- 7 If you are installing the firewall protection service over a previous installation, select **Restart** when prompted to reboot.

See also

[Prepare for installation on page 16](#)

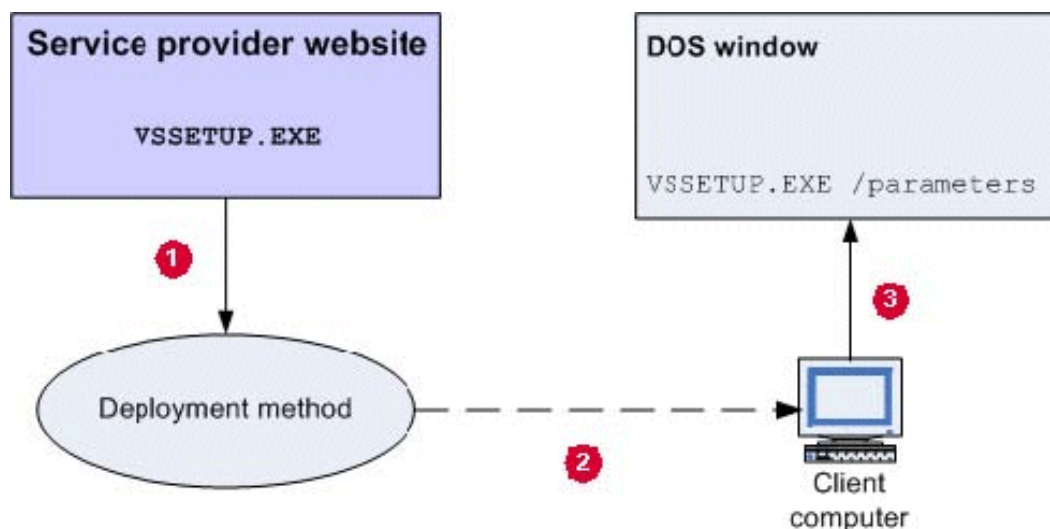
[Complete the installation on page 31](#)

The silent installation process

The silent installation method uses the executable file VSSETUP.EXE to install the client software with no user interaction. This installation method is not network-specific and installs the software on any Windows operating system.

How silent installation works

- 1 Download VSSETUP.EXE from the SecurityCenter.
- 2 Deploy to each computer where you want to install the client software.
- 3 On the computer, open a DOS window and run the VSSETUP.EXE command using the appropriate parameters.



Requirements for silent installation

Make sure you meet these requirements before using the silent installation method.

- You must have a method for installing executable files on your network computers. For example:
 - A third-party deployment tool, such as Novell NAL, ZenWorks, Microsoft Systems Management Server (SMS) installer, or Tivoli IT Director.
 - A login script.
 - A link to an executable file in an email message.
 - A portable medium such as a CD.
- You should run this program using an account with sufficient rights to install the product. Typically local administrator rights are required, and some methods require remote execution rights.
- You must know your company key (the series of characters in the installation URL after the characters CK=). The company key appears on the **Account & Keys** tab of the **My Account** page in the SecurityCenter.

Install with silent installation

Use this task to install the client software with the silent installation method.

Task

For option definitions, click ? in the interface.

- 1 In your web browser, log on to the SecurityCenter.
- 2 From the **Dashboard** or **Computers** page, click **Install Protection**.
- 3 Select **Desktop protection**, then click **Next**.
- 4 Under **Additional Installation Options**, select **Select advanced options**, then click **Silent install**.
The silent installation utility is downloaded to your computer.
- 5 Deploy the program to each client computer using your customary deployment tool.
- 6 Open a command prompt and run the following command on a client computer.

```
VSSETUP.EXE /CK=<your company key> /<parameters>
```

As shown in this example, you must include your company key (CK) as a parameter.



Your company key is included in the URL that you received when you subscribed to McAfee SaaS Endpoint Protection. It also appears on the **Accounts & Keys** tab of the **My Account** page in the SecurityCenter.

- 7 If you are installing the firewall protection service over an existing installation, reboot the client computer when prompted.

See also

[Complete the installation on page 31](#)

Designate a relay server with VSSETUP

Use this task to specify whether a computer should function as a relay server.

Task

For option definitions, click ? in the interface.

- Use a VSSETUP parameter to specify a computer as a relay server or change a relay server specification.

To do this...	Use this parameter
During installation, specify a computer is a relay server	VSSETUP /RelayServer=1  If you do not specify this parameter, the default is 0 and the computer is not a relay server.
Modify an existing installation to specify a computer is a relay server	VSSETUP /SetRelayServerEnable=1
Modify an existing installation to specify a computer is not a relay server	VSSETUP /SetRelayServerEnable=0

VSSETUP parameters

You can use several command line parameters when running the silent installation utility, vssetup.exe.

For a silent installation, use this command line and any of the following parameters (which are not case-sensitive):

```
VSSETUP.EXE /CK=<your company key> /<parameters>
```

Parameter	Description
/CK=XYZ	Required. Launches Setup using the company key. Your company key is listed on the SecurityCenter, on the Accounts & Keys tab of the My Account page.
/Email=x@y.com	Identifies the user's email address in administrative reports.  Despite its name, the email variable does not need to be an email address. This may also be a simple text identifier, e.g., location or computer name. However, do not use a string containing non-standard characters, because they might be displayed incorrectly in reports.
/Uninstall	Uninstalls McAfee SaaS Endpoint Protection.
/SetRelayServerEnable=1	Sets a computer with a connection to the Internet as a relay server. If the computer is not used as a relay server, set to 0.
/Reinstall	Re-installs McAfee SaaS Endpoint Protection, leaving the previous values for company key, email address, and machine ID intact.
/Groupid=[group number]	Places the computer into any group you have created. You can find the number associated with a group by checking the Computer Profiles report or by generating a customized URL. The group ID is at the end of the URL in the format G=xx.  If you designate a group that does not exist, users are placed in the Default Group or the group you have designated as your default group.
/Policyid=[policynumber]	Assigns a policy to the computer.  If you designate a policy that does not exist, the McAfee Default policy or the policy you have designated as your default is assigned.
/P=b /P=f /P=v	Selects the protection services to install: • b — browser protection • f — firewall protection • v — virus and spyware protection  If you omit the /P parameter, only the virus and spyware protection service is installed.
/ScanComputer	Performs a full scan on the computer as soon as installation is completed and detection definition (DAT) files are downloaded successfully.

```
VSSETUP.EXE /P=vfb /CK=abcd /Email=joe@example.com /Groupid=3
```

The virus and spyware protection, firewall protection, and browser protection services are installed. (If you purchased a version of McAfee SaaS Endpoint Protection that includes the web filtering module, it is installed with the browser protection service.) The company key is `abcd`, the user's email address is `joe@example.com` for reporting purposes, and the computer is placed in an existing group represented by the number 3. Check the **Computer Profiles** report to find the correct numeric groupid.

```
VSSETUP.EXE /CK=abcd /Email=joe@example.com
```

Only the virus and spyware protection service is installed. The company key is `abcd` and the user's email address is `joe@example.com` for reporting purposes. The computer is placed in the default group.

The push installation process

Push means deploying remotely to one or more computers in a network. This method uses the Push Install utility to deploy the client software to client computers on your network.

Push installation does not require third-party deployment software or interaction with users.

To perform a push installation:

- 1 Designate an *administrative computer*, where you will install the Push Install utility and initiate the push.
- 2 Select the *target computers*, which are client computers on your network that will receive the software.

The administrative computer and all the target computers must be in the same domain.

You can use the Push install utility to:

- Install client software on new network computers.
- Install client software on Active Directory groups.
- Install additional protection services on computers with existing client software.
- Select a large number of computers for installation, then customize some options for individual computers.
- Specify one or more computers that have an Internet connection as relay servers.

How push installation works

- 1 From the administrative computer, log on to the SecurityCenter, then download the Push Install utility from one of these locations:
 - As part of the **Install Protection** wizard, accessed from the **Dashboard** or **Computers** page.
 - From the **Installation** tab of the **Utilities** page.
- 2 Run the utility, select the target computers, and select installation options.
- 3 Initiate the push.

See also

[Decide whether to set up relay servers on page 14](#)

Requirements for push installation

You must meet these system requirements to deploy the client software using the push installation method.

Target computers

- Must be in the same Microsoft Windows domain as the administrative computer.

Administrative computer

- Must be running the Windows XP Professional, Windows Vista, Windows 7, or Windows 8 operating system.



Push installation is not supported on Microsoft Windows XP Home Edition because Windows XP Home Edition cannot log on to an Active Directory domain.

- Must have Version 2.0 of the Microsoft .NET Framework redistributable package installed.
- Must add **File and Print Sharing** to the firewall's **Exceptions** list when running the Windows firewall.
- Must have a supported web browser installed to access the SecurityCenter and download the file. (A browser is not required after the file is downloaded.)
 - Microsoft Internet Explorer (versions 7, 8, 9, and 10)
 - Mozilla Firefox (versions 3.0 through 15)
 - Google Chrome (versions 4.0 through 21)
 - Apple Safari for Windows (version 4.0, 5.0, and 5.1)

Administrator performing push installation

- Must have local system administrator privileges for the domain being installed.
- Must have credentials for logging on to the SecurityCenter. You received them in a Welcome email after you placed your order.

No separate login credentials are required if you do not rename the downloaded Push Install utility file and you begin the push installation within 20 minutes after downloading the file. Otherwise, you are prompted to log on to the SecurityCenter.

See also

[Active Directory support on page 15](#)

Considerations for scheduling push installations

Take these factors into account when scheduling push installations.

- **Consider other network tasks.** Pushing to a large number of computers simultaneously can produce a high volume of network traffic, so schedule push installations for times when they will not affect other network tasks.
- **Make sure the target computers are turned on.** The Push Install utility installs client software on target computers that are online and turned on when the push takes place.
- **Make sure users are not using the target computers.** Restarting a client computer while a push installation is in progress can cause the computer to become unstable. When installing the firewall protection service over an existing installation, the computers must be restarted, so schedule push installations for times when users will not be using their computers.

We recommend scheduling a push installation for the middle of the night, and sending users an email during the day asking them to leave their computers turned on overnight.

Install with push installation

Use this task to deploy the client software using the Push Install utility.



Back up any vital data on your critical servers before pushing software to them.

Task

For option definitions, click ? in the interface.

- 1 In your web browser, log on to the SecurityCenter.
- 2 From the **Dashboard** or **Computers** page, click **Install Protection**.
- 3 Select **Desktop protection**, then click **Next**.
- 4 Select **Use the Push Install utility**.
- 5 Click **Run Push Install utility**.
- 6 Enter your credentials.
 - Select **Use logged in user credentials** if you are logged in as the domain administrator.
 - Select **Use SSL only** if the domain has a certificate installed.
 - For the domain name, enter a domain name, the NETBIOS name of a domain, the IP address of a domain controller, or the NETBIOS name of a domain controller.
 - DNS and Active Directory are tied together. If you are installing to Active Directory groups, make sure that the system's primary DNS server is configured properly.
- 7 Select the target computers where you want to install the software and the appropriate options.
 - The policy to assign to the computers. If none is selected, the default policy is assigned.
 - The protection services to install.
 - Whether to scan the computer for threats when installation is complete. (*Recommended*)
- 8 To customize options for specific computers, click **Advanced**, select the appropriate options, then click **OK**. (*Optional*)
- 9 Select the computer for which you want to customize installation options, select the appropriate options, then click **OK**. (*Optional*)
 - The policy to assign to the computers. If none is selected, the default policy is assigned.
 - The protection services to install.
 - Whether to scan the computer for threats when installation is complete. (*Recommended*)
 - Whether to configure the computer as a relay server, which can distribute updates to other computers on the network.
- 10 Repeat step 9 for each computer you want to customize.
- 11 Click **Install Now**.

After installation is complete, a status for each target computer is displayed.

- 12 Click **View Log** to open a log file in Microsoft Notepad, which shows the status of the current session. The contents of the log file are deleted when you close the Push Install utility or perform another push installation.



The dialog box and log file indicate only whether the files were pushed to the target computers. It is important to review reports on the SecurityCenter or check the client computers to verify that the files were installed and the computers are updating successfully.

- 13 Restart the client computers. *(Required only if you have installed the firewall protection service over an existing installation.)*

See also

[Complete the installation on page 31](#)

Processes for pre-installed and CD versions

When the client software is pre-installed on a computer by the manufacturer or installed from a CD, you must activate the software and set up the account.

If your copy is...	Follow this process
Installed from a CD	To install the first copy: 1 Install using a CD. 2 Activate the software. 3 During the activation process, enter a license key to install the first copy and create an account. 4 After activation is complete, save the account enrollment key created by the Activation wizard. To install on additional computers: 1 Install using a CD. 2 Activate the software. 3 During the activation process, enter the account enrollment key. See the instructions that came with the CD for more information.
Pre-installed	1 Activate the software. 2 During the activation process, if a license key is required, enter the license key located on the McAfee license card shipped with your system. (Some PC makers do not require a license key. If no key is requested, skip this step.) 3 If it is a trial subscription, purchase a full subscription by the end of the trial period.

About pre-installed trial and full subscriptions

Pre-installed software comes in both trial and full subscriptions.

If a copy of McAfee SaaS Endpoint Protection is pre-installed on a computer, one of these options occurs the first time the computer is turned on:

- 1 A trial period begins. Activate the trial copy, evaluate the protection features, then purchase a full subscription to extend protection beyond the trial period.
- 2 A full subscription begins. Activate the subscription, then use the protection features until it is time to renew the subscription.

When you first turn on the computer

The first time a network is detected, a pre-installed copy of the McAfee SaaS Endpoint Protection client software updates the detection definition (DAT) files used to detect threats.

The on-access scanning feature then begins checking all files automatically as users access them, and they can perform on-demand scans to check all the files on their computer for threats. To continue receiving updates that protect against new threats, the client software must be activated.

In most cases, an activation reminder appears. If the client software is not activated, it stops functioning at the end of the activation period. When users attempt to access a feature, a notification reminds them that the activation period has ended and offers the opportunity to purchase a full subscription.

Activate the software

Activate a pre-installed or CD-based copy of McAfee SaaS Endpoint Protection to continue receiving DAT file updates against the latest threats. An activated copy checks for updates automatically at regular intervals.

Use this task to activate the software. This menu option is available only when activation is required.

Task

- 1 Click the product icon in the system tray, then select **Activate**.
- 2 In the Activation wizard, select the type of account to activate.

Option	Definition
Create a new account	If this is the first copy of the product that you are activating or purchasing, create a new account. Typically, the administrator selects this option. If you purchased multiple licenses, you can then add other computers to this account and manage security for all of them.
Join an existing account	Join an account that has already been set up.

- 3 Enter information to identify the account by following the instructions in the Activation wizard.

Purchase or renew a full subscription

After a trial subscription is activated, you can extend protection for the computer by purchasing a full subscription during the trial period.

A full subscription ensures that the computer continues to receive updates and retains access to features such as on-demand scans, automatic scanning of incoming email and attachments, monitoring of incoming communications for suspicious activity, and up-to-the-minute safety reports while browsing and searching the Internet.

When a full subscription nears expiration, you can renew it to ensure uninterrupted protection.

Use this task to purchase or renew a subscription. These menu options are available only when the status of the subscription requires attention.

Task

- 1 Click the product icon in the system tray, then select **Buy** or **Renew this Subscription**.
- 2 When prompted, enter the contact and payment information.



If a trial or full subscription has expired, McAfee SaaS Endpoint Protection is no longer protecting the computer. When you attempt to access a feature, a notification reminds you that the copy has expired and offers the opportunity to purchase or renew a full subscription.

View or create an account enrollment key

The account enrollment key is a unique identifier that enables you to add new installations of the client software to your account. It remains valid for seven days.

An account enrollment key is originally created when you activate a new account for a pre-installed copy or a CD version of McAfee SaaS Endpoint Protection. Then this key is required to:

- Activate new pre-installed copies of the client software under your account.
- Add new CD installations to your account.

If your key expires or is compromised, create a new one, which becomes effective immediately.

Use this task to view or create an account enrollment key.

Task

For option definitions, click ? in the interface.

- 1 On the SecurityCenter, check for an existing key on the **Accounts & Keys** tab of the **My Account** page.
- 2 If no current key is listed, click **Create a new key**.

Activate your license key after installation

If you do not have a valid license key when you install McAfee SaaS Endpoint Protection, set up a trial subscription to protect your computers while you obtain a license key.

Use this task to set up the trial, then obtain and activate a license key.

Task

For option definitions, click ? in the interface.

- 1 During the activation process, select **Continue as a trial user**.
- 2 From the SecurityCenter, on the **Accounts & Keys** tab of the **My Account** page, click **Activate License Key**.
- 3 Call the number listed for support to obtain a valid license key.
- 4 Enter the information requested in the form, then click **Next**.

Once you activate your license key, your account becomes a licensed full subscription. Licensing information is also updated automatically for other computers installed under your account.

Complete the installation

After installing McAfee SaaS Endpoint Protection, perform these tasks on each computer to ensure that the software is working correctly and the computer is protected.

Test virus protection

Use this task to test the virus-detection feature of the virus and spyware protection service by downloading the EICAR Standard AntiVirus Test File at the client computer.

Although it is designed to be detected as a virus, the EICAR test file is not a virus.

Task

- 1 Download the EICAR file from the following location:

<http://www.eicar.org/download/eicar.com>

If installed properly, the virus and spyware protection service interrupts the download and displays a threat detection dialog box.

- 2 Click **OK**.



If installed incorrectly, the virus and spyware protection service does not detect the virus or interrupt the download process. In this case, use Windows Explorer to delete the EICAR test file from the client computer, then re-install McAfee SaaS Endpoint Protection and test the new installation.

Scan the client computer

Use this task to scan the drives on a client computer after installing the virus and spyware protection service for the first time.

This scan checks for and cleans or deletes existing threats in files. In the future, files are scanned when they are accessed, downloaded, or saved.



If a full scan was performed as part of the installation process, you do not need to perform this task now. Ask your site administrator if you are unsure whether a scan has already been performed.

Task

- 1 Click the product icon in the system tray, then select **Open Console**.
- 2 From the **Action Menu**, select **Scan Computer**.
- 3 Select the scan target.

- **Scan my entire computer** — Scan all drives, folders, and files.



Mapped network drives are not scanned unless this feature is enabled in the policy assigned to the computer.

- **Scan a specific drive or folder** — Type the full path and name of the scan target or browse to locate it.

- 4 Click **Start Scan**.

The virus and spyware protection service displays the progress of the scan.



If needed, click **Pause Scan** to temporarily interrupt the scan or **Cancel Scan** to end the scan.

- 5 Click **View detailed report** to open a browser window and display the results of the scan.

Scan the email Inbox

Use this task to scan the contents of the Microsoft Outlook Inbox after installing the virus and spyware protection service for the first time.

This scan checks for threats in email already in the Inbox. Future emails are scanned before they are placed in the Inbox.

Task

- 1 In the Microsoft Outlook Inbox, highlight one or more messages in the right pane.
- 2 Under **Tools**, select **Scan for Threats**.

The **On-Demand Email Scan** dialog box appears when the scan starts. From the dialog box, you can stop, pause, and restart the scan. You can also check the results of the scan.

2

Troubleshooting and reference

This section contains information to help resolve problems you might encounter when installing the product.

Contents

- ▶ *Troubleshooting tasks*
- ▶ *Frequently asked questions*
- ▶ *Error messages*

Troubleshooting tasks

Use these tasks at the client computer to help resolve installation problems.

Tasks

- *Troubleshoot general installation problems on page 33*
Use this task to resolve problems that do not generate an error message during installation.
- *Uninstall the client software on page 34*
Use this task at a client computer to remove the client software.

Troubleshoot general installation problems

Use this task to resolve problems that do not generate an error message during installation.

If you are not able to identify and resolve the problem after each step, proceed to the next step.

Task

- 1 Run the McAfee Virtual Technician wizard.

Launch the tool from <http://mvt.mcafee.com> and follow the instructions on the screen. See [TS101111](#) for download links and detailed instructions on using this tool. During the process, you will need to download the diagnostic tool if it is not already installed.

The tool scans the computer, diagnoses and fixes problems, replaces missing or corrupted registry keys, restarts any stopped McAfee services, and checks for known issues and missing update packages. If the tool is unable to fix the problem, it creates a log that describes the problems, so that you can attempt to fix them, and a session report that technical support can retrieve if needed.

- 2 Check that the computer meets the system requirements described in this document.

- 3 Check the McAfee Support KnowledgeBase to see if the problem is documented there.

For a quick-reference listing of KB articles related to many common issues, including installation and uninstallation, see [KB75932](#).

- 4 Uninstall the software. You can use the Windows **Add/Remove Programs** feature, or proceed to the next step and run the **Cleanup** utility to uninstall the software (which requires administrator credentials).
Even if the installation failed, some components of the client software might have been installed. Uninstalling the software ensures these are removed.
- 5 Download and run the **Cleanup** utility (also called the uninstall utility, mvsuninst.exe). This step requires administrative credentials for the SecurityCenter. If you do not have them, ask your site administrator for assistance, or skip to the next step.
The utility is available on the SecurityCenter, on the **Migration & Optimization** tab of the **Utilities** page. See [KB55238](#) for instructions on using the utility to remove any extra registry files and other components that might have been left behind.
- 6 Download and run the pre-installation utility.
See [KB75738](#) for the downloadable file and instructions for using it.
The utility verifies that your system meets the minimum requirements, performs some general cleanup tasks like clearing the browser cache, and performs some general checks and tests. It creates a report with details about any issues it finds.
- 7 If you are still unable to install the client software, ask your site administrator to contact technical support.

See also

[System requirements on page 11](#)

[How firewall protection interacts with the Windows firewall on page 14](#)

[Support for corporate firewalls or proxy servers on page 15](#)

[Terminal server support on page 15](#)

Uninstall the client software

Use this task at a client computer to remove the client software.

You might need to do this for testing purposes or before re-installing the client software. (Note that some protection services, such as the SaaS protection services, do not include a client software component.)



This task uses the Windows feature for uninstalling software, which does not always remove all the associated components, such as registry keys. A McAfee utility is available that cleans up these components, and you can also use it to uninstall the software. This **Cleanup** utility requires administrative credentials for the SecurityCenter, and is available on **Migration & Optimization** tab of the **Utilities** page.

If you uninstall the client software, the computer is no longer protected. We recommend that you re-install as soon as possible.

Task

- 1 Close the Microsoft Outlook and Internet Explorer applications.
- 2 In the Windows Control Panel, open **Add/Remove Programs** or **Programs and Features**.

3 Select the protection services uninstall, then click **Remove** or **Uninstall**.

- McAfee Virus and Spyware Protection Service
- McAfee Firewall Protection Service
- McAfee Browser Protection Service



On computers running the Windows firewall, the setting for the Windows firewall is automatically restored to the setting that was in effect before the client software was installed. If the Windows firewall was enabled then, it is re-enabled automatically now.

See also

Troubleshoot general installation problems on page 33

Frequently asked questions

Here are answers to frequently asked questions.



The most current information on product-related questions is documented in the McAfee Support online KnowledgeBase. For a quick-reference listing of popular KB articles, see [KB75932](#).

Questions about installation

Does it matter which email address or identifier I enter when installing the client software?

No. Any description can be entered in the field, or it can be left blank. However, an email address provides a link for notifying the principal user about security issues for the computer. The information entered identifies the client computers in administrative reports.

While installing the client software, the installation process appears to stop responding.

The installation might take a few minutes to complete. However, if the status bar stops moving and nothing in the installation window has changed in more than five minutes, close the window and start the installation process again (for example, by clicking the installation URL).

Do access protection or behavior blocking rules in other applications affect installation of the client software?

Yes. If users are unable to install the client software and you have defined access protection or behavior blocking rules, such as those that would prevent binaries from executing from the Temp folder, disable them and try installing again.

I want to update the Microsoft Windows operating system on my client computer. Do I need to re-install the client software?

Yes. If you upgrade a client computer's operating system (for example, from Windows XP to Windows 7) and you want to leave your existing files and programs intact during the upgrade, you must first uninstall the client software, then re-install it after the upgrade is complete.

Questions about pre-installed and CD-based software

Why should I activate each copy of the client software?

The first time a user turns on a computer with a pre-installed copy of the product or installs it from a CD, the computer is updated with the latest detection definition (DAT) files and product components. No more updates occur until the copy is activated. To ensure that the computer is always protected against the latest threats, activate the copy as soon as possible.

How can I protect a computer while I purchase additional licenses?

Install the software as a trial. Then purchase additional licenses and merge the trial account into your main account.

What if I can't find my license key or the key is not valid?

If you do not have a valid license key when you install the product, you can obtain one and register it later. Install it as a trial to ensure that the computer is protected while you obtain a license key, then activate the license key.

How do I know when new installations of McAfee SaaS Endpoint Protection have joined my account? Do I need to perform any setup tasks for them?

An alert appears on the **Dashboard** page of the SecurityCenter to notify you when new computers have been added. By default, new computers are placed in the **Default Group** and assigned the **McAfee Default** policy. If you want to change these settings, click the resolution button for the alert to display instructions. If you do not want to change these settings, select **Dismiss Alert**.

Error messages

Error messages are displayed by programs when an unexpected condition occurs that can't be fixed by the program itself. Use this list to find an error message, an explanation of the condition, and any action you can take to correct it.

Installation

A file needed to install the software is not available. Please click the installation URL to begin the installation process again.

When a user clicks the installation URL to download the installation file using Microsoft Internet Explorer, a cookie is created in Internet Explorer. The cookie expires after 24 hours. If the user saves the installation file and then tries to install it after 24 hours have passed, or deletes the cookie, that user must download the file and begin the installation process again.

Installation cannot proceed because you have selected not to accept a vital agent component, you don't have administrative rights to your machine, or other issues occurred.

This error message can be caused by several different problems:

- **The security level of the browser is too high.** Set the browser's security level to a level where Javascript is enabled. In Internet Explorer, the default setting of **Medium** or **Medium-high** is sufficient.
- **A registry file is missing.** The system file Regedit.exe might be missing. Search for that file in the client computer's \Windows folder. If the file is missing, replace it by using the original Windows install media or copy it from another computer that is running the same operating system.
- **The browser cache is full.** Empty the browser cache. See the browser's documentation for instructions.

Installation Declined.

This message can appear after a failed installation or uninstallation of the client software. It indicates that leftover product files need to be removed from the client computer. Remove these components by downloading and running the Cleanup utility on the computer where you need to install. (Or ask the site administrator for assistance. This utility is available on the **Migration & Optimization** tab of the **Utilities** page on the SecurityCenter.)

Installation Denied.

Common causes and solutions:

- When you begin the installation, Microsoft Internet Explorer displays a dialog box asking you to verify that you want to install McAfee SaaS Endpoint Protection. You must click **Yes**.
- The Windows system file Regedit.exe must be present in the Windows directory. If it is missing, replace it by using the original Windows install media or copy it from another computer that is running the same operating system.

Invalid Entitlement Error.

The installation URL in your email message might have been truncated or badly formatted. Make sure that you are using the entire URL with no spaces, and that the company key at the end of the URL is complete. You might need to paste the URL into your web browser if you cannot select it from your email message. (The company key is the value after the characters CK=. A site administrator can verify that a company key is correct on the **Accounts & Keys** tab of the **My Account** page on the SecurityCenter.)

This error can also indicate that the trial evaluation period or subscription has expired, or that you are attempting to install protection on more computers than licenses have been purchased for. Check the SecurityCenter for information about the status of your subscriptions and licenses, or ask the administrator for assistance.

MyASUtil.SecureObjectFactory error message.

The SecureObjectFactory Class program might have become corrupted. To verify this, check the status of the SecureObjectFactory Class program file.

- 1 Launch Internet Explorer.
- 2 From the **Tools** menu, select **Internet Options**.
- 3 In the **Temporary Internet Files** section of the dialog box, click **Settings** to display the **Settings** dialog box.
- 4 Click **View Objects** to open the **Downloaded Program Files** folder.
- 5 Find the entry for **SecureObjectFactory Class**. Make note of the information in the **Status** and **Creation Date** columns:
 - If the status and dates are listed as **Unknown**, delete the **SecureObjectFactory Class** program file. Uninstall and re-install the client software to reload the file.
 - If the status is listed as **Installed**, with valid dates, the file is not damaged.
 - If there is another comment in the **Status** column, contact your administrator or product support with that information.



If you do not see a **Status** column, set your view options to **Details**.

MyINX Error.

The installer has detected other virus protection software on the computer, which you must uninstall.

- 1 From the Windows Control Panel, open **Add/Remove Programs** or **Programs and Features**.
- 2 In the list of programs, locate any virus protection software (other than McAfee SaaS Endpoint Protection), then click **Remove** or **Uninstall**.
- 3 Begin the installation process again.

If you have uninstalled McAfee SaaS Endpoint Protection and still receive this error, some components might be installed but not visible, because the installation was only partially completed. Remove these components by downloading and running the Cleanup utility on the computer where you need to install. (Or ask the site administrator for assistance. This utility is available on the **Migration & Optimization** tab of the **Utilities** page on the SecurityCenter.)

Unable to create Cab Installer Object.

One possible cause is that the service MyAgtSvc.exe is no longer running on the computer. You must manually restart it.

- 1 Select **Start | Run**.
- 2 Type the path to MyAgtSvc.exe (you can use **Browse** to locate the file) and add the option /start. For example: c:\program files\McAfee\Managed VirusScan\Agent\myagtsvc.exe /start
- 3 Click **OK**.

If that does not solve the problem, contact your administrator or product support.



This is a Microsoft Internet Explorer error, and might require installing a Microsoft patch.

Cannot find remote shared directory.

This error appears during a failed push installation. The target computers did not meet one or more of the following requirements:

- **File and Print Sharing** must be enabled.
- User-level access control must be configured.
- They must not be running Microsoft Windows XP Home Edition, which does not support Windows NT Domain logins.
- The person initiating the push must have domain administrator rights.

Check if the client computer you are pushing to has the appropriate shares enabled, and if you have appropriate administrator rights to perform a push installation to that computer. To check:

- 1 On the client computer, select **Start | Run**.
- 2 In the **Open** text box, type \\CPUNAME\ADMIN\$ (where CPUNAME is the name of the computer to which you are pushing); then click **OK**.

The \Windows directory of the computer to which you are trying to push should be displayed. If you do not have sufficient administrator rights to that computer, or if that computer does not have appropriate user-level access and sharing enabled, a **Network path not found** error dialog box appears.

- 3 See your Windows networking documentation for information on fixing your network administrative settings.

Active Directory

Active Directory user does not have sufficient privileges to perform a remote installation.

The credentials entered for the Active Directory server do not allow you to install software remotely. Check with your IT administrator or contact McAfee technical support for assistance.

Invalid Active Directory credentials were provided.

The credentials entered for the Active Directory server were not valid. Check with your IT administrator or contact McAfee technical support for assistance.

Index

64-bit support
 firewall protection service [11](#)

A

about this guide [5](#)
account enrollment key
 defined [30](#)
 viewing or creating [30](#)
accounts
 merging multiple accounts [10](#)
activation
 license key [30](#)
 pre-installed software [29](#)
 trial software [29](#)
Active Directory [18](#)
 installing on Active Directory groups [15](#)
 push installation and [25](#)
Add/Remove Programs
 removing other firewall programs [16](#)
 removing other virus protection [16](#)
administrative computers
 defined [25](#)
 installing client software on [19](#)
 requirements for push installation [26](#)
administrator rights
 client software installation and [17](#), [19](#), [22](#)
 domain, push installation and [26](#)
 terminal servers and [15](#)
anti-virus applications, removal of [16](#)
Apple Safari, *See* Safari browser
authentication, support for [15](#)
automatic updates
 after installation [20](#)
 proxy servers and [15](#)

B

browser requirements
 browser protection [11](#)
 general [11](#)
 push installation [26](#)

C

CD version of software
 requirements for [28](#)
CHAP proxy [15](#)
Chrome
 browser protection and [11](#)
Cleanup utility [33](#), [34](#)
client computers
 browser requirements [11](#)
 operating system requirements [11](#)
 requirements for push installation [26](#)
 scanning after installation [31](#)
 scanning Outlook Inbox after installation [32](#)
 system requirements [11](#)
client software
 deploying by push installation [25](#), [27](#)
 deploying by silent installation [22](#)
 deploying to Active Directory groups [15](#)
 installation methods [18](#)
 installing on administrative computer [19](#)
 testing installation of [31](#)
 uninstalling [34](#)
command-line parameters, silent installation with VSSETUP [24](#)
company key, installation and [22](#)
configuration of browser for installation [11](#)
conventions and icons used in this guide [5](#)
conversion of trial to full subscription [29](#)
create
 account enrollment key [30](#)
 customized installation URL [20](#)
customize
 options for push installation [27](#)
 options for silent installation [24](#)
 URL for installation [20](#)

D

default firewall [14](#)
deployment tools
 for silent installation [22](#)
 for standalone installation agent [17](#)
deployment, client software
 push installation [27](#)
 silent installation [22](#)

deployment, standalone installation agent [17](#)

disable

Windows firewall [14](#)

documentation

audience for this guide [5](#)

online Help [6](#)

product and user guides [6](#)

product-specific, finding [6](#)

typographical conventions and icons [5](#)

viewing [6](#)

domains, push installation and [26, 27](#)

downloads

Active Directory Synchronization utility [15](#)

Cleanup utility [33](#)

pre-installation utility [16, 33](#)

Push Install utility [25](#)

standalone installation agent [17](#)

uninstall utility [33](#)

VSSETUP utility [22](#)

E

EICAR test virus [31](#)

email addresses

entering during installation [20](#)

entering during order process [10](#)

multiple accounts and [10](#)

email scans (virus and spyware protection), on-demand scan [32](#)

email server protection, installation requirements [13](#)

error messages [36](#)

F

fast user switching, support for [15](#)

Firefox

browser protection and [11](#)

firewall

Windows 7 [34](#)

Windows 8 [34](#)

Windows Vista [34](#)

Windows XP [34](#)

firewall protection

rebooting computer after installation [22, 27](#)

supported operating systems [11](#)

uninstalling existing firewall software [16](#)

Windows firewall and [14](#)

firewalls

corporate, support for [15](#)

default [14](#)

setting up [14](#)

uninstalling existing firewall software [16](#)

Windows [14, 16](#)

G

Google Chrome, *See* Chrome

grant number [10](#)

H

help

viewing [6](#)

I

installation

Active Directory and [15](#)

administrator rights [17](#)

browser requirements [11](#)

corporate network firewall and [15](#)

entering email address [20](#)

methods of [18](#)

pre-installation utility [16](#)

preparing to install [16](#)

procedure [20](#)

proxy server and [15](#)

push, overview [25](#)

requirements [11](#)

requirements for pre-installed or CD software [28](#)

requirements, general [11](#)

silent, overview [22](#)

standalone installation agent [17](#)

testing [31](#)

troubleshooting [33](#)

uninstalling existing firewall software [16](#)

uninstalling existing virus protection software [16](#)

URL, overview [19](#)

User Account Control dialog box [20](#)

users without administrator rights [17](#)

without a license key [30](#)

installation URL, creating or obtaining [18, 20](#)

Internet Explorer

browser protection and [11](#)

L

license key [30](#)

licenses

buying [29](#)

renewing [29](#)

log files, for Windows firewall [14](#)

M

McAfee ServicePortal, accessing [6](#)

McAfee Virtual Technician [33](#)

Microsoft Exchange Server 2003 [13](#)

Microsoft Exchange Server 2007 [13](#)

Microsoft Internet Explorer, *See* Internet Explorer

Mozilla Firefox, *See* Firefox

multiple accounts, merging [10](#)

mvsuninst utility [33](#)

N

non-Microsoft browsers [11](#)

notifications, about operating system support [12](#)
 NTLM proxy [15](#)

O

on-demand scans
 client computers [31](#)
 email (virus and spyware protection) [32](#)
 online Help, viewing [6](#)
 operating systems
 requirements for email server protection [13](#)
 requirements for push installation [26](#)
 requirements for URL installation [19](#)
 support for [11](#)
 upgrading [11](#)
 Outlook Inbox, scanning [32](#)

P

pre-installation utility [16](#), [33](#)
 pre-installed software
 activating [29](#)
 requirements for [28](#)
 processor requirements [11](#)
 proxy servers [15](#)
 purchase of full subscription [29](#)
 push installation
 Active Directory support [25](#)
 administrative computers [25](#)
 downloading utility [25](#)
 enabling relay servers [27](#)
 overview [18](#), [25](#)
 procedure [27](#)
 proxy server and [15](#)
 requirements [26](#)
 restarting client computers after [27](#)
 scheduling considerations [26](#)
 target computers [25](#)

R

RAM requirements [12](#)
 relay servers
 overview of [14](#)
 push installation and [27](#)
 silent installation and [23](#)
 removal of
 existing firewall software [16](#)
 existing virus protection software [16](#)
 renewal of subscriptions [29](#)
 reports, identifying computers in [20](#)
 requirements
 browser [11](#)
 CD versions [28](#)
 email server protection [13](#)
 operating system [11](#)
 pre-installed software [28](#)

requirements (*continued*)
 push installation [26](#)
 RAM [12](#)
 SaaS email protection [13](#)
 server operating systems [11](#)
 silent installation [22](#)
 URL installation [19](#)
 restart for client computers [22](#), [27](#)

S

Safari browser, browser protection and [11](#)
 scans
 client computers, after installation of client software [31](#)
 mapped network drives and [31](#)
 Outlook Inbox, after installation of client software [32](#)
 viewing results [31](#)
 security level, browser [11](#)
 servers
 requirements for client software installation [11](#)
 requirements for email server protection [13](#)
 ServicePortal, finding product documentation [6](#)
 silent installation
 company key [22](#)
 deployment tools for [22](#)
 diagram [22](#)
 enabling/disabling relay servers [23](#)
 overview [18](#), [22](#)
 procedure [22](#)
 proxy server and [15](#)
 requirements for [22](#)
 VSSETUP command-line parameters [24](#)
 standalone installation agent
 defined [17](#)
 deploying [17](#)
 subscriptions, purchase and renewal [29](#)
 support for
 browsers [11](#)
 fast user switching [15](#)
 operating systems [11](#)
 relay servers [14](#)
 terminal servers [15](#)
 Windows firewall [14](#)

T

target computers
 defined [25](#)
 requirements for push installation [26](#)
 restarting after push installation [27](#)
 Technical Support, finding product information [6](#)
 terminal servers, support for [15](#)
 test
 virus protection (virus and spyware protection) [31](#)
 trial subscriptions
 activating [29](#)

trial subscriptions (*continued*)
 converting to full subscription [29](#)
 creating when license key unavailable [30](#)
 troubleshooting, installation problems [33](#)

U

uninstall utility [33](#), [34](#)
 uninstallation
 client software [34](#)
 client software, troubleshooting [33](#)
 existing firewall software [16](#)
 existing virus protection software [16](#)
 updates
 after installation [20](#)
 proxy server and [15](#)
 upgrades for client operating system [11](#)
 URL installation
 creating or obtaining URL [18](#), [20](#)
 overview [19](#)
 procedure [20](#)
 requirements for [19](#)
 sending URL to users [20](#)
 User Account Control dialog box [20](#)
 utilities
 Active Directory Synchronization utility [15](#)
 Cleanup utility [33](#), [34](#)
 McAfee Virtual Technician [33](#)
 pre-installation utility [16](#), [33](#)
 Push Install utility [25](#), [27](#)
 standalone installation agent, defined [17](#)
 uninstall utility [33](#), [34](#)
 VSSETUP, defined [22](#)

V

virus and spyware protection
 scanning client drives after installation [31](#)

virus and spyware protection (*continued*)
 scanning Outlook Inbox after installation [32](#)
 testing virus protection [31](#)
 uninstalling existing virus protection software [16](#)

VSSETUP utility
 command-line parameters for [24](#)
 defined [22](#)
 downloading [22](#)
 enabling/disabling relay servers [23](#)
 running [22](#)

W

what's in this guide [6](#)
 Windows 7
 fast user switching support [15](#)
 firewall [14](#), [16](#), [34](#)
 push installation, administrative computer and [26](#)
 Windows 8
 firewall [14](#), [34](#)
 Windows firewall
 disabling [14](#)
 firewall protection service and [14](#)
 log file location [14](#)
 Windows Vista
 fast user switching support [15](#)
 firewall [14](#), [16](#), [34](#)
 push installation, administrative computer and [26](#)
 Windows XP
 fast user switching support [15](#)
 firewall [14](#), [16](#), [34](#)
 firewall protection service and [11](#)
 push installation, administrative computer and [26](#)
 Windows XP Home Edition and push installation [26](#)

